Technical Cybersecurity

More Scanning!

Other Scans

STEALTH SCAN

- `$ nmap -oN stealth.txt -sS 172.16.248.*`

ACK SCAN

- `$ nmap -oN ack.txt -sA 172.16.248.*`

Try the others. Do you see any differences?

Try this.

```
$ nmap -oN mystery.txt -Pn -sS 172.16.248.*
```

Wow! Lots more info.

MORE DETAILED

- This is a scan looking at services available on hosts rather than just seeing which hosts exist.

SERVICES

- Some hosts have more services than others.
- Which host has the most exposed services? which has the least?

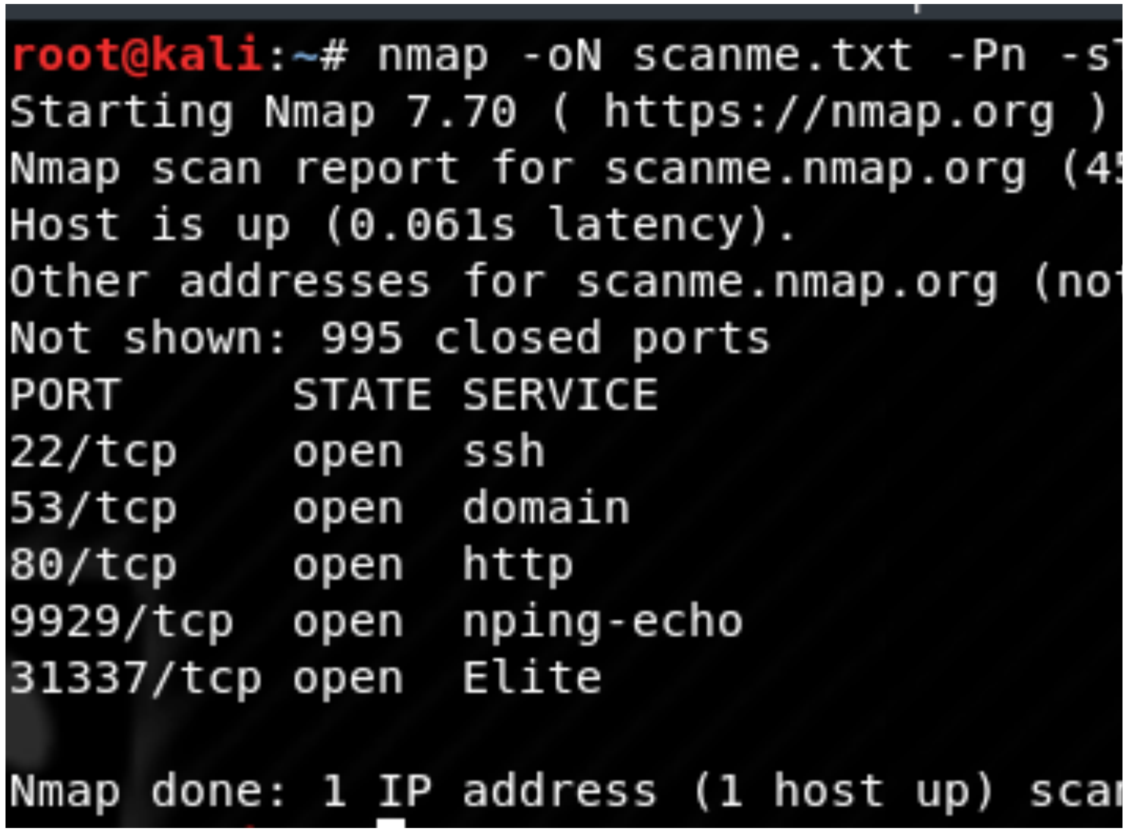
Details

LET'S HIT SCANME

- **$ nmap -oN scanme.txt -Pn -sT scanme.nmap.org**
- **$ nmap -oN scanme-udp.txt -sU scanme.nmap.org**

SERVICES

- 53 is DNS (this is UDP)
- 22 is SSH
- 80 is HTTP
- 31337 is Elite (?)
- 123 is NTP (this is UDP)



```
root@kali:~# nmap -oN scanme.txt -Pn -sT
Starting Nmap 7.70 ( https://nmap.org )
Nmap scan report for scanme.nmap.org (45
Host is up (0.061s latency).
Other addresses for scanme.nmap.org (not
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scan
```

(https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml)

Try other options v.
scanme and in your lab.

Next, we’ll talk about more detailed recon and then pull back to DNS and other methods.